J. Symbolic Computation (1997) **24**, 575–589

Solving a Multivariable Congruence by Change of Term Order

PATRICK FITZPATRICK†

Department of Mathematics, University College, Cork, Ireland

We consider the congruence $a \equiv \sum_{i=1}^{s} b_i h_i \bmod I$ where $h_1, \ldots, h_s$ are given modulo a zero dimensional ideal I. We give two polynomial time algorithms for determining a Gröbner basis, relative to an arbitrary term order, of the module M of solutions of the congruence, and, in particular, for finding its minimal element. These are based on a generalization of an algorithm of Faugère *et al.* and extend the 1-variable solution techniques that use the Euclidean algorithm and the Berlekamp–Massey algorithm.

1. Introduction

In Fitzpatrick and Flynn (1992), we considered the general problem of Padé approximation as the solution of the congruence

$$a \equiv bh \bmod I \tag{1.1}$$

where I is an ideal in $A = F[x_1, \ldots, x_n]$, represented in terms of a Gröbner basis $\mathcal{I} = \{p_j, 1 \leq j \leq m\}$ relative to an arbitrary, fixed term order $<$ in A, and h is a given polynomial in normal form relative to $\mathcal{I}$. Often, a, b are to be determined subject to specified conditions: for example, when I is generated by the set of homogeneous terms of total degree d, we may require relatively prime a, b satisfying the total degree condition:

$$\deg(a) \leq \ell_1, \deg(b) \leq \ell_2, \text{ and } \ell_1 + \ell_2 < d.$$

More generally we are interested in solving

$$a \equiv \sum_{i=1}^{s} b_i h_i \bmod I \tag{1.2}$$

where $h_1, \ldots, h_s$ are given polynomials in normal form relative to $\mathcal{I}$.

We showed that the solution module $M = \{(a, b) | a \equiv bh \bmod I\}$ of (1.1) has a basis $\mathcal{U} = \{(h, 1), (p_j, 0), 1 \leq j \leq m\}$ which is a Gröbner basis relative to the term order $<_\omega$ in A^2 induced from $<$ by the weight vector $\omega = (1, \mathrm{Lt}(h))$, with $\mathrm{Lt}(h)$ denoting the leading term of h relative to $<$. A similar result holds for the solution module of (1.2)—see Theorem 3.1. A solution (a, b) is *minimal* relative to a term order in A^2 if its leading

† E-mail: fitzpat@ucc.ie

0747–7171/97/110575 + 15 $25.00/0 sy970153

term is minimal; such a solution is clearly unique up to multiplication by a constant. Under conditions such as the term order condition, we proved that the required solution is the minimal element in M relative to a new term order $<_{\omega'}$ induced from $<$ by another weight vector ω'. For example, if $<$ is a degree order with x_n largest among the variables then the term order condition leads to $\omega' = (x_n^{\ell_2}, x_n^{\ell_1})$. Since any Gröbner basis must contain the minimal solution, it may be found by calculating a Gröbner basis $\mathcal{U}'$ of M relative to this new term order. Under certain weaker conditions the required solution is the minimal *reduced* solution, defined by the property that both a, b are reduced relative to $\mathcal{I}$. In this case the required solution lies in the reduced Gröbner basis with respect to a new term order, but it may not be the minimal element.

In this paper we propose algorithms for determining Gröbner bases of the solution module M of (1.2), relative to arbitrary term orders in the case that I is a zero dimensional ideal. We take as our starting point the algorithm of Faugère *et al.* (1993) (often denoted by the initials FGLM) whose purpose is to convert a Gröbner basis for a zero dimensional ideal of A with respect to one term order into a Gröbner basis with respect to another. In Section 2 we give the (straightforward) generalization of this algorithm to submodules of finite codimension in A^r, where for our application $r = s + 1$. The solution module M of (1.2) has this property when I is zero dimensional. In Section 3 we describe the simplifications that may be made to the generalized FGLM algorithm in the determination of Gröbner bases of M.

An alternative approach to the solution of (1.2), for the special case in which I is generated by terms, is to use the sequences of coefficients of h_i to construct the required basis via a sequence of modules M_ℓ solving the successive approximation problems

$$a \equiv \sum_{i=1}^{s} b_i h_i \bmod I_\ell \tag{1.3}$$

where $\langle 1 \rangle = I_0 > I_1 > \cdots > I_N = I$ is such that $I_\ell = \langle \varphi_\ell, I_{\ell+1} \rangle$ for some term $\varphi_\ell \in A$. This "iterative" algorithm is presented in Section 4.

In both algorithms the minimal element is the first to be inserted into the new basis, and if this is the only solution required the algorithm may be halted as soon as it has appeared.

The problem of determining a minimal solution of (1.1) (for various definitions of minimality) appears in a number of different applications. For example, the 1-variable case arises in the decoding problem for alternant codes: this has been analyzed in Fitzpatrick (1995). The specializations of these algorithms to 1-variable polynomials lead to procedures similar in form to the extended Euclidean algorithm and improving on the Berlekamp–Massey algorithm. Thus our techniques may be regarded as extending the classical algorithms to the case of n variables. In Section 5 we give examples of applications to the determination of multivariable Padé approximants with prescribed numerator and denominator degrees and to the decoding of certain geometric Goppa codes.

2. Generalized FGLM Algorithm

There are two ways of developing the theory of Gröbner bases of submodules of $A^r = F[x_1, \ldots, x_n]^r$. In Adams and Loustauneau (1994, Chapter 3), the theory is developed directly using the vectors in A^r. In Becker and Weispfenning (1993, Section 10.5), it is shown that the theory may be regarded as a special case of the theory of homogeneous Gröbner bases in $F[x_1, \ldots, x_n, z_1, \ldots, z_r]$, where the auxiliary variables z_i take the place

of the standard basis vectors. In this paper we use the former approach which seems more natural for our purposes, in particular for the term orders we require (see Theorem 3.1, Theorem 5.1). In one case (Example 5.5) we shall briefly refer to the alternative formulation to define a term order according to the general construction using a matrix of real vectors given by Robbiano (1985).

We define a term in A to be a power product, without coefficient attached, and define a term in A^r as an element of the form $t = \varphi \boldsymbol{e}_k, 1 \leq k \leq r$ where φ is a term in A, and $\boldsymbol{e}_k$ a standard basis vector (of length r with a single non-zero entry equal to 1 in the kth component). The set of terms in A^r is denoted by $\mathcal{T}_r$ and each element of A^r may be expressed in component form as $\sum_{k=1}^{r} a_k \boldsymbol{e}_k, a_k \in A$. The term $\varphi \boldsymbol{e}_k$ is a nontrivial multiple of $\psi \boldsymbol{e}_k$ if there is a term $\psi' \in \mathcal{T}_1$ with $\varphi \boldsymbol{e}_k = \psi'(\psi \boldsymbol{e}_k)$; the term $\varphi \boldsymbol{e}_k$ cannot be a multiple of $\psi \boldsymbol{e}_\ell$ for any $\ell \neq k$.

A term order in A^r is a total order $<$ on $\mathcal{T}_r$ with the properties (i) $t < \psi t$ for all $t \in \mathcal{T}^r, \psi \in \mathcal{T}_1, \psi \neq 1$, and (ii) if $t_1 < t_2$, $t_i \in \mathcal{T}_r$, then $\psi t_1 < \psi t_2$ for all $\psi \in \mathcal{T}_1$. For a given term order on $\mathcal{T}_r$, the leading term of an element $p \in A^r$ is denoted by $\mathrm{Lt}(p)$ and the set of leading terms of any set $\mathcal{P}$ of elements is denoted by $\mathrm{Lt}(\mathcal{P})$. It will be clear from the context what the value of r is and which order is being invoked.

Let $N \subseteq A^r$ be a submodule and denote by $\mathrm{Nf}_{\mathcal{U}}(p)$ the normal form of $p \in A^r$ relative to a Gröbner basis $\mathcal{U}$ of N. If N has finite codimension then there are only finitely many terms that are reduced modulo N. The object of the basis conversion algorithm is to use a Gröbner basis of N with respect to one term order to derive a Gröbner basis relative to a new term order. The method is a generalization of the algorithm of Faugère *et al.* (1993).

Let $\mathcal{U}_1$ be a Gröbner basis of N with respect to the term order $<_1$ and let $<_2$ be a second term order. The algorithm that follows constructs

a Gröbner basis $\mathcal{U}_2$ of N relative to $<_2$,
a list *lead_terms* of the leading terms of $\mathcal{U}_2$,
a list *red_terms* of the terms that are reduced with respect to $\mathcal{U}_2$.

For use within the algorithm we also require

a list *terms_tbc* (terms to be considered),
a procedure *order*($\mathcal{S}$) that puts a list $\mathcal{S}$ of terms into ascending order with respect to $<_2$, and removes any duplicates,
a procedure *append*($\mathcal{S}, t$) that appends to a list $\mathcal{S}$ the list $[x_i t, 1 \leq i \leq n]$ for a given term t,
a procedure *next*($\mathcal{S}$) that removes the first term from the list $\mathcal{S}$ and returns its value.

Initially, *red_terms* contains the smallest term with respect to $<_2$; this is necessarily of the form $1\boldsymbol{e}_k$ for some $k, 1 \leq k \leq r$ (if not, it has the form $\varphi \boldsymbol{e}_k$ and then $\varphi \boldsymbol{e}_k < 1\boldsymbol{e}_k$ which contradicts the fact that the term order is a well-ordering). The list *terms_tbc* is initialized to an ordered list of all the other terms of the form $1\boldsymbol{e}_k$. At each iteration a term t is removed from *terms_tbc* and, if it is not a multiple of an element already in *lead_terms*, then writing $\mathrm{Nf}_1(p) = \mathrm{Nf}_{\mathcal{U}_1}(p)$, we determine whether $\mathrm{Nf}_1(t)$ can be written as a linear combination of the normal forms of the terms in *red_terms*. If so, it leads to a new element of $\mathcal{U}_2$ and is placed in *lead_terms*; otherwise it is inserted in *red_terms*. More formally, we state the algorithm as follows.

ALGORITHM 2.1. (GENERALIZED FGLM)

Input
Gröbner basis $\mathcal{U}_1$ of $N \subseteq A^r$ relative to a term order $<_1$, where N has finite codimension
Term order $<_2$

Output
Reduced Gröbner basis $\mathcal{U}_2$ of N relative to $<_2$
List *lead_terms* of leading terms of $\mathcal{U}_2$ in ascending order relative to $<_2$
List *red_terms* of terms in normal form with respect to $\mathcal{U}_2$ in ascending order relative to $<_2$

Initialize
$t :=$ least term in T_r relative to $<_2$;
red_terms $:= [t]$; *terms_tbc* $:=$ *order*$([1\boldsymbol{e}_k, 1 \le k \le r | 1\boldsymbol{e}_k \ne t])$;
$\mathcal{U}_2 := [\,]$; *lead_terms* $:= [\,]$;
append(*terms_tbc*, t);
order(*terms_tbc*);

Main program
while *terms_tbc* $\ne [\,]$ do
  $t :=$ *next*(*terms_tbc*)
  if t is not a nontrivial multiple of an element in *lead_terms* then
    if there exists a linear equation
      $\mathrm{Nf}_1(t) = \sum_{v \in red\_terms} \alpha_v \mathrm{Nf}_1(v)$, $\alpha_v \in F$
    then
      $\mathcal{U}_2 := \mathcal{U}_2 \cup \{t - \sum_{v \in red\_terms} \alpha_v v\}$
      lead_terms $:=$ *lead_terms* $\cup \{t\}$
    else
      red_terms $:=$ *red_terms* $\cup \{t\}$
      append(*terms_tbc*, t)
      order(*terms_tbc*)

PROOF. The proof of the algorithm is an extension of that in Faugère *et al.* (1993). It is obvious that the normal forms (with respect to $\mathcal{U}_1$) of the elements in *red_terms* are linearly independent, otherwise we could derive a relation contradicting the definition of a particular term as being in *red_terms*. Since N has finite codimension, the number of terms in *red_terms* is bounded. Note that each iteration of the main loop begins by removing a term from *terms_tbc* and further terms are inserted in *terms_tbc* only in the event that *red_terms* is also enlarged. Thus at each step either the size of *terms_tbc* decreases or the size of *red_terms* increases. This implies that there are only a finite number of iterations.

Next, $\mathcal{U}_2 \subseteq N$, since for any element we have

$$\mathrm{Nf}_1\Big(t - \sum_{v \in red\_terms} \alpha_v v\Big) = 0.$$

Clearly, t is the leading term of this element.

Finally, let $\varphi \boldsymbol{e}_k$ be any term that is not placed in *red_terms*. If $1\boldsymbol{e}_k \in$ *lead_terms* then $\varphi \boldsymbol{e}_k$ is a multiple of an element in *lead_terms*. Otherwise, $1\boldsymbol{e}_k \in$ *red_terms* and we can consider the maximal term $\psi \boldsymbol{e}_k \in$ *red_terms* of which $\varphi \boldsymbol{e}_k$ is a (necessarily nontrivial) multiple. Thus there is a $\psi' \neq 1$ in $\mathcal{T}_1$ with $\varphi \boldsymbol{e}_k = \psi'(\psi \boldsymbol{e}_k)$. This means that there is some variable x_i such that $x_i \psi \boldsymbol{e}_k$ appeared in *terms_tbc*, $x_i \psi \boldsymbol{e}_k \notin$ *red_terms*, and $\varphi \boldsymbol{e}_k$ is a multiple of $x_i \psi \boldsymbol{e}_k$. We conclude that $\varphi \boldsymbol{e}_k$ is a multiple of an element of *lead_terms*. Consequently, on completion, every term not in *red_terms* is a multiple of an element of *lead_terms* and hence is contained in $\langle \mathrm{Lt}(\mathcal{U}_2) \rangle$. Now the leading term with respect to $<_2$ of any element $u \in \mathcal{U}_1$ cannot be in *red_terms* since $\mathrm{Nf}_1(u) = 0$. It follows that $\mathrm{Lt}(u) \in \langle \mathrm{Lt}(\mathcal{U}_2) \rangle$ and hence that $\mathcal{U}_2$ is a Gröbner basis of N with respect to $<_2$. It is clear that *lead_terms* and *red_terms* are ordered lists of terms with the required properties. This completes the proof of the algorithm. □

By construction, $\mathcal{U}_2$ is reduced since in each of its elements every term apart from the leading term is reduced.

It is clear that the complexity of this algorithm is the same as that of FGLM—the reader is referred to Faugère *et al.* (1993) for a detailed analysis.

THEOREM 2.2. *Let N be a submodule of finite codimension $D(N)$ in A^r and let $\mathcal{U}_1$ be a Gröbner basis of N relative to a term order $<_1$. Then a reduced Gröbner basis $\mathcal{U}_2$ of N relative to another term order $<_2$ can be calculated in $\mathcal{O}(nD(N)^3)$ arithmetic operations.*

PROOF. The construction of each normal form $\mathrm{Nf}_1(t)$ required can be carried out in $\mathcal{O}(D(N)^2)$ operations and the new basis comprises at most $nD(N)$ elements. The linear algebraic computation required by the algorithm is essentially the triangularization of an $nD(N) \times D(N)$ matrix. □

When the algorithm is used to find only the minimal element, at most $D(N) + 1$ rows of the matrix of normal forms need to be examined before a linear dependence is found. Thus we have

COROLLARY 2.3. *The minimal element of N relative to an arbitrary term order $<_2$ can be calculated using Algorithm 2.1 in $\mathcal{O}(D(N)^3)$ arithmetic operations.*

In considering the computational complexity a distinction must be made between fields in which arithmetic operations have a unit cost and those in which the cost varies with the size of the representation of the input and intermediate computations. Again there is no essential difference between the ideal and the module cases—the reader is referred to Faugère *et al.* (1993) for details.

3. Solving Congruences

Our concern here is with the special case of Algorithm 2.1 when it is used to determine a Gröbner basis of the solution module M of (1.2).

We require a special type of term order in A^r defined as follows. Let $<$ be an arbitrary, fixed term order in $\mathcal{T}_1$ and let $\omega = (\omega_1, \ldots, \omega_r) \in \mathcal{T}_1^r$. The term order $<_\omega$ on $\mathcal{T}_r$ is defined by the condition $\varphi \boldsymbol{e}_i <_\omega \psi \boldsymbol{e}_j$ if either $\varphi\omega_i < \psi\omega_j$ or ($\varphi\omega_i = \psi\omega_j$ and $i < j$), and $\psi \boldsymbol{e}_j <_\omega \varphi \boldsymbol{e}_i$ otherwise (see Möller and Mora, 1986).

A "natural" basis of M is given in the following theorem, which is a consequence of Möller and Mora (1986, Theorem 7.8) (see also Fitzpatrick and Flynn (1992, Theorem 2.1)).

THEOREM 3.1. *Let $M \subseteq A^r, r = s+1$ be the solution module of (1.2) and let $\mathcal{I}$ be a Gröbner basis of I relative to a term order $<$ in A. Then*

$$\mathcal{U} = \{h_k \boldsymbol{e}_1 + 1\boldsymbol{e}_k \mid 2 \le k \le r\} \cup \{p_j \boldsymbol{e}_1 \mid p_j \in \mathcal{I}\}$$

is a Gröbner basis of M with respect to the term order $<_\omega$ defined by $<$ and $\omega = (1, \mathrm{Lt}(h_1), \ldots, \mathrm{Lt}(h_s))$.

This follows easily from the fact that under $<_\omega$ the leading terms of $h_k \boldsymbol{e}_1 + 1\boldsymbol{e}_k, p_j \boldsymbol{e}_1$ are $1\boldsymbol{e}_k$ and $p_j \boldsymbol{e}_1$ respectively.

The next result describes normal forms relative to $\mathcal{U}$; the straightforward proof is left as an exercise.

THEOREM 3.2. *Let $\mathcal{U}$ be the basis of M given in Theorem 3.1.*

(i) *Each term $\varphi \boldsymbol{e}_1$ with $\varphi \notin \mathrm{Lt}(I)$ is reduced relative to $\mathcal{U}$.*
(ii) *The normal form of $\psi \boldsymbol{e}_k, 2 \le k \le r$, relative to $\mathcal{U}$ is $\psi \boldsymbol{e}_k - \psi(h_k \boldsymbol{e}_1 + 1\boldsymbol{e}_k)$ reduced modulo $\mathcal{I}$, that is, $\mathrm{Nf}_{\mathcal{U}}(\psi \boldsymbol{e}_k) = \mathrm{Nf}_{\mathcal{I}}(-\psi h_k)\boldsymbol{e}_1$.*
(iii) *The normal form of $(a, b_1, \ldots, b_s) \in A^r$ relative to $\mathcal{U}$ is $\mathrm{Nf}_{\mathcal{I}}(a - \sum_{i=1}^s b_i h_i)\boldsymbol{e}_1$.*

Since the terms that are reduced modulo $\mathcal{U}$ are precisely those of the form $\varphi \boldsymbol{e}_1$ with $\varphi \notin \mathrm{Lt}(I)$ we have

COROLLARY 3.3. *The codimension of M is the codimension $D(I)$ of I.*

As a consequence the implementation of Algorithm 2.1 in the determination of a basis of M may be carried out using a table of normal forms of terms *modulo* $\mathcal{I}$ and hence the complexity is reduced accordingly.

COROLLARY 3.4. *A reduced Gröbner basis of M relative to an arbitrary term order $<_2$ can be calculated using Algorithm 2.1 in $\mathcal{O}(nD(I)^3)$ arithmetic operations. The minimal element of M can be calculated in $\mathcal{O}(D(I)^3)$ arithmetic operations.*

4. An Iterative Algorithm

In this section we consider determining a Gröbner basis of the solution module M of (1.2) relative to a term order $<_2$ using the sequence of approximating modules M_ℓ defined in (1.3). There are various possibilities for the descending sequence of ideals I_ℓ; we assume that for each ℓ, $0 \le \ell \le N$, we have a given Gröbner basis $\mathcal{I}_\ell$ of I_ℓ relative to some fixed term order $<$. The essential property required for the algorithm that follows is

$$I_\ell = \langle \varphi_\ell, \mathcal{I}_{\ell+1} \rangle \tag{4.1}$$

for some term $\varphi_\ell \in \mathcal{T}_1$. For instance, in the case of two variables x, y, if I is generated by the terms of a given total degree, and the underlying term order $<$ in $\mathcal{T}_1$ is total degree

lexicographic with $x < y$, then we may define the sequence $\mathcal{I}_\ell$ as follows:

$$\begin{aligned}\mathcal{I}_0 &= \{1\}\\ \mathcal{I}_1 &= \{x, y\}\\ \mathcal{I}_2 &= \{y, x^2\}\\ \mathcal{I}_3 &= \{x^2, xy, y^2\}\end{aligned}$$

and so on, and set $I_\ell = \langle \mathcal{I}_\ell \rangle$. In this example, $\varphi_0 = 1, \varphi_1 = x, \varphi_2 = y$, etc.

Throughout this section we write Nf_ℓ for $\mathrm{Nf}_{\mathcal{I}_\ell}$. It follows from Theorem 3.1 that

$$\mathcal{U} = \{\mathrm{Nf}_\ell(h_k)\boldsymbol{e}_1 + 1\boldsymbol{e}_k \mid 2 \le k \le r\} \cup \{p_j \boldsymbol{e}_1 \mid p_j \in \mathcal{I}_\ell\} \tag{4.2}$$

is a Gröbner basis of M_ℓ with respect to the term order $<_\lambda$ defined by

$$\lambda = (1, \mathrm{Lt}(\mathrm{Nf}_\ell(h_1)), \ldots, \mathrm{Lt}(\mathrm{Nf}_\ell(h_s))).$$

In order to be able to pass from one approximating module to the next we need to have a fixed ordering of the terms. This is provided by the following lemma.

LEMMA 4.1. *The set $\mathcal{U}$ defined in* (4.2) *is a Gröbner basis of M_ℓ with respect to the term order $<_\omega$ defined by*

$$\omega = (1, \mathrm{Lt}(h_1), \ldots, \mathrm{Lt}(h_s)).$$

PROOF. The given set is obviously still a basis of M_ℓ. Also, the leading terms relative to $<_\omega$ of $\mathrm{Nf}_\ell(h_k)\boldsymbol{e}_1 + 1\boldsymbol{e}_k, p_j\boldsymbol{e}_1$ are $1\boldsymbol{e}_k, p_j\boldsymbol{e}_1$ respectively. These clearly generate the leading term of any element of M_ℓ where this is in any position other than the first. If $(a, b_1, \ldots, b_s)$ has leading term $\mathrm{Lt}(a)\boldsymbol{e}_1$ then we have

$$\mathrm{Lt}(a) > \mathrm{Lt}(b_i)\,\mathrm{Lt}(h_i), 1 \le i \le s.$$

Since $(a, b_1, \ldots, b_s)$ can be reduced by subtracting basis elements to $(a - \sum_{i=1}^s b_i h_i)\boldsymbol{e}_1$, it follows that $a - \sum_{i=1}^s b_i h_i \equiv 0 \bmod I_\ell$. But, by the equation above, $\mathrm{Lt}(a - \sum_{i=1}^s b_i h_i) = \mathrm{Lt}(a)$ so $\mathrm{Lt}(a) \in I_\ell$. This completes the proof. □

We shall consider an element $w = (a, b_1, \ldots, b_s)$ of a basis $\mathcal{W}_\ell$ of M_ℓ as a candidate for inclusion in a basis $\mathcal{W}_{\ell+1}$ of $M_{\ell+1}$. For w to be contained in $M_{\ell+1}$ it is necessary and sufficient that the coefficient of φ_ℓ in the nonzero (first) component of the normal form of w relative to $\mathcal{I}_{\ell+1}$ be zero (cf. Theorem 3.2(iii)). We will refer to this loosely as the coefficient of φ_ℓ in $\mathrm{Nf}_{\ell+1}(w)$ and denote it by $\alpha_\ell(w)$. It follows from Theorem 3.2(iii) that $\alpha_\ell(w)$ is the coefficient of φ_ℓ in the expansion of $a - \sum_{i=1}^s b_i h_i$.

In order to motivate the algorithm and clarify its proof, we first compare the application of Algorithm 2.1 to $\mathcal{U}_\ell$ with its application to $\mathcal{U}_{\ell+1}$. For convenience, we refer to these instances as $\mathrm{NB}(\ell), \mathrm{NB}(\ell+1)$, respectively (NB stands for "new basis") and denote the bases thus determined by $\mathcal{V}_\ell, \mathcal{V}_{\ell+1}$.

The sequences of terms considered in $\mathrm{NB}(\ell)$ and $\mathrm{NB}(\ell+1)$ are the same, namely, the terms $\mathcal{T}_r$ (with $r = s+1$) ordered according to $<_2$. For the argument that follows it is convenient to take a slightly different conceptual view of Algorithm 2.1 than that actually implemented. We suppose the list $\mathcal{T}_r$ known in its entirety *ab initio* and consider it term by term. As each term t is considered it is deleted from $\mathcal{T}_r$, and one of the following operations is carried out:

(1) t is placed in the set of leading terms of (new) basis elements; all multiples of t are deleted from $\mathcal{T}_r$ and inserted in a set of "excluded" terms,
(2) t is placed in the set of reduced terms.

Thus each application of NB partitions $\mathcal{T}_r$ into three subsets, namely the reduced, leading, and excluded terms. We denote the subsets generated by $\mathrm{NB}(\ell), 0 \le \ell \le N$, by $\mathcal{R}(\ell), \mathcal{L}(\ell), \mathcal{E}(\ell)$ respectively. Our aim is to identify the difference between $\mathcal{L}(\ell)$ and $\mathcal{L}(\ell+1)$. This is analyzed in the following sequence of results.

LEMMA 4.2.

(i) $\mathcal{L}(\ell+1) \cap \mathcal{R}(\ell) = \emptyset$.
(ii) $\mathcal{L}(\ell+1) \subseteq \mathcal{L}(\ell) \cup \mathcal{E}(\ell)$.
(iii) $\mathcal{L}(\ell) \subseteq \mathcal{L}(\ell+1) \cup \mathcal{R}(\ell+1)$.

PROOF. A linear relation among normal forms relative to $\mathcal{I}_{\ell+1}$ restricts to a linear relation relative to $\mathcal{I}_\ell$ so if $\rho \boldsymbol{e}_j \in \mathcal{L}(\ell+1)$ then there is a linear relation expressing $\mathrm{Nf}_\ell(\rho \boldsymbol{e}_j)$ in terms of normal forms of earlier terms. This implies that either $\rho \boldsymbol{e}_j \in \mathcal{L}(\ell)$ or $\rho \boldsymbol{e}_j$ has already been eliminated from consideration as a multiple of an element in $\mathcal{L}(\ell)$. In any case it does not lie in $\mathcal{R}(\ell)$ and (i) follows. Statement (ii) is a straightforward consequence. Note that this implies that each element of $\mathcal{L}(\ell+1)$ is a multiple of some element of $\mathcal{L}(\ell)$. Finally, if an element of $\mathcal{L}(\ell)$ were in $\mathcal{E}(\ell+1)$ then it would be a multiple of an element of $\mathcal{L}(\ell+1)$ and therefore, by (ii), a multiple of an element of $\mathcal{L}(\ell)$—this is a contradiction. □

LEMMA 4.3. *If $\mathcal{L}(\ell) \subseteq \mathcal{L}(\ell+1)$ then $\mathcal{L}(\ell) = \mathcal{L}(\ell+1)$ and $\mathcal{R}(\ell) = \mathcal{R}(\ell+1)$.*

PROOF. Suppose $\mathcal{L}(\ell) \subseteq \mathcal{L}(\ell+1)$ and consider a term $\mathcal{L}(\ell+1)$. This cannot be in $\mathcal{R}(\ell)$ by Lemma 4.2(i). By definition, it cannot be a nontrivial multiple of another term in $\mathcal{L}(\ell+1)$, so it cannot be a nontrivial multiple of a term in $\mathcal{L}(\ell)$. Thus it does not lie in $\mathcal{E}(\ell)$ so by Lemma 4.2(ii) it lies in $\mathcal{L}(\ell)$. It follows that $\mathcal{L}(\ell+1) = \mathcal{L}(\ell)$; consequently, $\mathcal{E}(\ell+1) = \mathcal{E}(\ell)$ and $\mathcal{R}(\ell+1) = \mathcal{R}(\ell)$. □

The alternative possibility is that there is a least term in $\mathcal{L}(\ell)$ which is placed in $\mathcal{R}(\ell+1)$ by $\mathrm{NB}(\ell+1)$.

LEMMA 4.4. *Let $\sigma \boldsymbol{e}_k$ be minimal such that $\sigma \boldsymbol{e}_k \in \mathcal{L}(\ell) \cap \mathcal{R}(\ell+1)$.*

(i) *If $\rho \boldsymbol{e}_j <_2 \sigma \boldsymbol{e}_k$ then $\rho \boldsymbol{e}_j \in \mathcal{L}(\ell+1)$ if and only if $\rho \boldsymbol{e}_j \in \mathcal{L}(\ell)$.*
(ii) $\{x_i \sigma \boldsymbol{e}_k, 1 \le i \le n\} \subseteq \mathcal{L}(\ell+1) \cup \mathcal{E}(\ell+1)$.
(ii) *If $\sigma \boldsymbol{e}_k <_2 \rho \boldsymbol{e}_j$ then $\rho \boldsymbol{e}_j \in \mathcal{L}(\ell)$ implies $\rho \boldsymbol{e}_j \in \mathcal{L}(\ell+1)$ while $\rho \boldsymbol{e}_j \in \mathcal{L}(\ell+1)$ implies either $\rho \boldsymbol{e}_j \in \mathcal{L}(\ell)$ or $\rho \boldsymbol{e}_j = x_i \sigma \boldsymbol{e}_k$ for some i, $1 \le i \le n$.*

PROOF. Note first that by definition the coefficient $\alpha_\ell(\sigma \boldsymbol{e}_k)$ is nonzero, otherwise $\sigma \boldsymbol{e}_k$ would be in $\mathcal{L}(\ell+1)$ by Lemma 4.2(iii).

(i) Let $\rho \boldsymbol{e}_j <_2 \sigma \boldsymbol{e}_k$, and suppose first that $\rho \boldsymbol{e}_j \in \mathcal{L}(\ell)$. By the definition of $\sigma \boldsymbol{e}_k$, $\rho \boldsymbol{e}_j \notin \mathcal{R}(\ell+1)$, so $\rho \boldsymbol{e}_j \in \mathcal{L}(\ell+1)$ by Lemma 4.2(iii). Conversely, suppose $\rho \boldsymbol{e}_j \in \mathcal{L}(\ell+1)$. If $\rho \boldsymbol{e}_j \notin \mathcal{L}(\ell)$ then $\rho \boldsymbol{e}_j \in \mathcal{E}(\ell)$ by Lemma 4.2(ii). This implies that $\rho \boldsymbol{e}_j$ is a nontrivial

multiple of an element of $\mathcal{L}(\ell)$ less than $\sigma \boldsymbol{e}_k$. But, by the previous paragraph, all such terms lie in $\mathcal{L}(\ell+1)$ so $\rho \boldsymbol{e}_j$ is a nontrivial multiple of an element of $\mathcal{L}(\ell+1)$ and therefore lies in $\mathcal{E}(\ell+1)$, a contradiction.

(ii) If $m \in M_\ell$ is the element with leading term $\sigma \boldsymbol{e}_k$ then $x_i m \in M_{\ell+1}$ since $x_i \varphi_\ell \in I_{\ell+1}$. Hence $x_i \sigma \boldsymbol{e}_k \notin \mathcal{R}(\ell+1)$.

(iii) Let $\sigma \boldsymbol{e}_k <_2 \rho \boldsymbol{e}_j$, and suppose first that $\rho \boldsymbol{e}_j \in \mathcal{L}(\ell)$. If $\alpha_\ell(\rho \boldsymbol{e}_j) = 0$ then the linear relation defining $\rho \boldsymbol{e}_j$ as an element of $\mathcal{L}(\ell)$ still holds. This implies that $\rho \boldsymbol{e}_j \notin \mathcal{R}(\ell+1)$, so $\rho \boldsymbol{e}_j \in \mathcal{L}(\ell+1)$ by Lemma 4.2(iii). On the other hand if $\alpha_\ell(\rho \boldsymbol{e}_j) \neq 0$ then

$$\alpha_\ell \left(\rho \boldsymbol{e}_j - \frac{\alpha_\ell(\rho \boldsymbol{e}_j)}{\alpha_\ell(\sigma \boldsymbol{e}_k)} \sigma \boldsymbol{e}_k \right) = 0.$$

Thus, the linear relations defining $\rho \boldsymbol{e}_j$ and $\sigma \boldsymbol{e}_k$ as elements of $\mathcal{L}(\ell)$ may be combined to give a linear relation defining $\rho \boldsymbol{e}_j$ as an element of $\mathcal{L}(\ell+1)$. Conversely, suppose $\rho \boldsymbol{e}_j \in \mathcal{L}(\ell+1)$. Then, by Lemma 4.2(ii), $\rho \boldsymbol{e}_j \in \mathcal{L}(\ell) \cup \mathcal{E}(\ell)$. If $\rho \boldsymbol{e}_j \in \mathcal{E}(\ell)$ then it is a nontrivial multiple of an element of $\mathcal{L}(\ell)$ not contained in $\mathcal{L}(\ell+1)$. By (i) and the previous paragraph, the only candidate is $\sigma \boldsymbol{e}_k$ and now (ii) applies. □

REMARK 4.5. Part (ii) of this lemma implies that $\mathrm{NB}(\ell+1)$ is complete as soon as $\{x_i \sigma \boldsymbol{e}_k\}$ have been considered.

We now have the following theorem which provides the idea behind the iterative algorithm.

THEOREM 4.6. *Either $\mathcal{L}(\ell+1) = \mathcal{L}(\ell)$ or there is a least term $\sigma \boldsymbol{e}_k$ under $<_2$ such that $\sigma \boldsymbol{e}_k \in \mathcal{L}(\ell) \cap \mathcal{R}(\ell+1)$. In the latter case $\mathcal{L}(\ell+1) = (\mathcal{L}(\ell) \setminus \{\sigma \boldsymbol{e}_k\}) \cup \{x_i \sigma \boldsymbol{e}_k, 1 \le i \le n\}$, with the understanding that any element of $\{x_i \sigma \boldsymbol{e}_k, 1 \le i \le n\}$ that is a multiple of an element of $\mathcal{L}(\ell)$ is omitted.*

The algorithm is initialized with the set $\mathcal{W}_0 = \{1\boldsymbol{e}_k, 1 \le k \le r\}$ which is a Gröbner basis of $M_0 = A^r$ relative to any term order. In the ℓth iteration the elements of $\mathcal{W}_\ell$ are ordered in increasing order of leading term (with respect to $<_2$) and any element whose leading term is a multiple of another leading term is rejected. The algorithm calculates the coefficient $\alpha_{\ell j} = \alpha_\ell(\mathrm{Nf}_{\ell+1}(\mathcal{W}_\ell[j]))$ of φ_ℓ in the normal form of $\mathcal{W}_\ell[j]$ relative to $\mathcal{U}_{\ell+1}$ (we use $\mathcal{S}[j]$ to denote the jth element of the list $\mathcal{S}$). If this is zero then $\mathcal{W}_\ell[j] \in M_{\ell+1}$, and it is retained as an element of the new basis $\mathcal{W}_{\ell+1}$ being constructed, that is, $\mathcal{W}_{\ell+1}[j] = \mathcal{W}_\ell[j]$. Otherwise, let q be the smallest index for which $\alpha_{\ell q} \neq 0$. Then $\mathcal{W}_\ell[q]$ is replaced by $\{x_i \mathcal{W}_\ell[q], 1 \le i \le n\}$ and, for all $j > q$ we define $\mathcal{W}_{\ell+1}[j] = \mathcal{W}_\ell[j] - (\alpha_{\ell j}/\alpha_{\ell q})\mathcal{W}_\ell[q]$ (this makes no change if $\alpha_{\ell j} = 0$). If any of the elements of $\mathcal{W}_{\ell+1}$ has leading term a multiple of the leading term of another element then it is omitted, since (as we show) the basis derived at each stage is a Gröbner basis. In practice the only possibility is that one of $\{x_i \mathcal{W}_\ell[q]\}$ has this property since these are the only elements whose leading terms are not already in $\mathrm{Lt}(\mathcal{W}_\ell)$.

We denote the number of elements in a set $\mathcal{S}$ by $|\mathcal{S}|$. The procedure *order*($\mathcal{S}$) (slightly modfied from Algorithm 2.1) has two functions, namely, to put the elements of a list $\mathcal{S} \subseteq A^r$ in ascending order of leading term with respect to $<_2$, and to remove any element whose leading term is a multiple of the leading term of another element (if two elements have identical leading terms only one of them is removed—preferably the most recently generated).

ALGORITHM 4.7. (ITERATIVE SOLUTION MODULE)

Input
Sequence of ideals and terms satisfying (4.1) with $I_N = I$.
Polynomials $h, p_1, \ldots, p_s$ reduced modulo I.
Term order $<_2$.

Output
Gröbner basis $\mathcal{W}$ of the solution module M of (1.2)
relative to $<_2$.

Initialize
$\ell := 0$; $\mathcal{W} := order([1\boldsymbol{e}_k, 1 \le k \le r = s+1])$

Main program
while $\ell < N$ do
  for j from 1 to $|\mathcal{W}|$ do
    $\alpha_{\ell j} := \alpha_\ell(\mathrm{Nf}_{\ell+1}(\mathcal{W}[j]))$
  $q :=$ least j for which $\alpha_{\ell j} \neq 0$
  replace $\mathcal{W}[q]$ by $[x_i\mathcal{W}[q], 1 \le i \le n]$
  for j from q to $|\mathcal{W}|$ do
    $\mathcal{W}[j] := \mathcal{W}[j] - (\alpha_{\ell j}/\alpha_{\ell q})\mathcal{W}[q]$
  order($\mathcal{W}$)
  $\ell := \ell + 1$

PROOF. We use notation developed prior to the statement of the algorithm. Initially, $\mathcal{W}$ is a basis for $M_0 = A^r$, which is a Gröbner basis with respect to any term order. Moreover, it is the basis that would be determined by Algorithm 2.1. Suppose, by induction, that $\mathrm{Lt}(\mathcal{W}_\ell) = \mathcal{L}(\ell)$, that is, $\mathrm{Lt}(\mathcal{W}_\ell)$ is the same as the set of leading terms that would be found by applying Algorithm 2.1 to $\mathcal{U}_\ell$. This implies that $\mathcal{W}_\ell$ is a Gröbner basis of M_ℓ relative to $<_2$. We claim that $\mathrm{Lt}(\mathcal{W}_{\ell+1}) = \mathcal{L}(\ell+1)$.

Since subtraction of a constant multiple of an element with lower leading term does not change the leading term of the minuend, $\mathrm{Lt}(\mathcal{W}_{\ell+1})$ is identical to $\mathrm{Lt}(\mathcal{W}_\ell)$ apart from the exclusion of $\mathrm{Lt}(\mathcal{W}_\ell[q])$ and the inclusion of $x_i\,\mathrm{Lt}(\mathcal{W}_\ell[q])$, for $1 \le i \le n$, up to removal of redundant elements. Thus we need only prove that $\mathrm{Lt}(\mathcal{W}_\ell[q]) = \sigma\boldsymbol{e}_k$, as defined in Theorem 4.6. By the induction hypothesis $\mathrm{Lt}(\mathcal{W}_\ell[q]) \in \mathcal{L}(\ell)$ and it is clear that $\mathrm{Lt}(\mathcal{W}_\ell[q]) \notin \mathcal{L}(\ell+1)$, so $\mathrm{Lt}(\mathcal{W}_\ell[q]) \in \mathcal{R}(\ell+1)$ by Lemma 4.2(iii). But, by construction, every element of $\mathcal{L}(\ell)$ that comes before $\mathrm{Lt}(\mathcal{W}_\ell[q])$ lies in $\mathcal{L}(\ell+1)$. Consequently, $\mathrm{Lt}(\mathcal{W}_\ell[q])$ is the minimal element in $\mathcal{L}(\ell) \cap \mathcal{R}(\ell+1)$ and this completes the proof. □

REMARKS 4.8.

(i) In order to eliminate unnecessary calculations when only the minimal element is required, the algorithm does not necessarily produce a reduced basis at each stage. A reduction step can easily be added if required.
(ii) The minimal element in M can be calculated without determining the full Gröbner basis of M by modifying the algorithm so that at each iteration the current minimal element $(a, b_1, \ldots, b_s)$ is checked to determine the largest value of ℓ for which it belongs to M_ℓ. As soon as the current minimal element lies in M, it is the minimal

element of M, since any further subtractions of multiples of other basis elements would only serve to increase its leading term. Thus no further iterations of the algorithm are necessary.

(iii) The relationship between Algorithms 2.1 and 4.7 is precisely that between the extended Euclidean algorithm and the Berlekamp–Massey algorithm techniques for the solution of the 1-variable versions of (1.1). Indeed, the restrictions of Algorithms 2.1 and 4.7 to $F[x]$ give algorithms similar in form to the classical ones and thus they may be regarded as n-variable generalizations (see Fitzpatrick, 1995).

We conclude this section by considering the complexity of the iterative algorithm. It is easy to see that at the ℓth iteration the number of elements in the basis is at most $r+(n-1)\ell$, and since each basis element contains r polynomials with at most ℓ non-zero coefficients the updating step requires $\mathcal{O}(n\ell^2)$ arithmetic operations. Consequently, for the determination of the full basis the algorithm has complexity $\mathcal{O}(nD(I)^3)$. On the other hand, it is not easy to estimate in general the complexity of the algorithm when it is used to determine only the minimal element. This is because it does not seem possible to predict in advance how many iterations are necessary before the minimal element of M becomes the current minimal element. In practice, examples show that the algorithm improves on Algorithm 2.1 for finding the minimal element when this is "small", that is, when it satisfies a condition such as the total degree condition mentioned in the Introduction (see also the next section).

5. Applications

The basic problem corresponding to (1.1) is that of Padé approximation in A. Here we are given the expansion of h as far as total degree d and required to find (a,b) satisfying the total degree condition $\deg(a) \le \ell_1, \deg(b) \le \ell_2$ where $\ell_1 + \ell_2 < d$. The following condition is weaker than the total degree condition and includes it as a special case (cf. Fitzpatrick and Flynn, 1992).

weak term order condition: Let $<$ be a term order on $\mathcal{T}_1$ and suppose that

(i) there exist $\varphi, \psi \in \mathcal{T}_1$ such that $\mathrm{Lt}(a) \le \varphi, \mathrm{Lt}(b) \le \psi$,

(ii) for all $\rho, \sigma \in \mathcal{T}_1$ with $\rho \le \varphi, \sigma \le \psi$ and $\rho, \sigma \notin \mathrm{Lt}(I)$ the product $\rho\sigma$ does not lie in $\mathrm{Lt}(I)$.

Then we say that a, b satisfy $\mathrm{wtoc}(\varphi, \psi, <)$.

We assume that a Gröbner basis $\mathcal{I}$ of I is given and call a solution (a,b) *reduced* if both a and b are in normal form relative to $\mathcal{I}$. We then have

Theorem 5.1. (Fitzpatrick and Flynn, 1992; Theorem 2.4) *Suppose that there is a reduced solution (a,b) of Eqn (1.1) with a, b relatively prime and satisfying* $\mathrm{wtoc}(\varphi, \psi, <)$. *Then (a,b) is the unique minimal reduced element (defined up to a constant multiple) of the solution module M and, as a consequence, it appears in the reduced Gröbner basis of M relative to the term order $<_\omega$ defined by $\omega = (\psi, \phi)$.*

For example, if $<$ is total degree lexicographic with $x_1 < \cdots < x_n$ then the total degree condition mentioned in the Introduction leads to consideration of the term order $<_\omega$ defined by $\omega = (x_n^{\ell_2}, x_n^{\ell_1})$.

It may happen that the minimal reduced solution is actually the minimal element in M: for example, this is always the case under the total degree condition. It is worthwhile to clarify when this occurs.

COROLLARY 5.2. *Let (a, b) be the minimal reduced element of M relative to an arbitrary term order $<$. Then either (a, b) is the minimal element of M relative to $<$ or the minimal element has the form $(p, 0)$ or $(0, q)$ for some p or q in I.*

PROOF. If (a, b) is not minimal then the minimal element has the form (a', b') with $\mathrm{Lt}(a', b') < \mathrm{Lt}(a, b)$ and by definition (a', b') is not reduced. By reducing a', b' modulo I we obtain a reduced element (a'', b'') with $\mathrm{Lt}(a'', b'') \leq \mathrm{Lt}(a', b')$ and hence $(a'', b'') = (0, 0)$. It follows that $(a', b') = (p, q)$ for some $p, q \in I$. But $(p, 0), (0, q)$ also both lie in M and one of these has leading term lower than $\mathrm{Lt}(p, q)$. The lemma now follows. □

EXAMPLE 5.3. We consider finding the Padé approximant (a, b) for $h = 3x^3 + x^2y + 2y^3 + 5x^2 + 6xy + y^2 + 6x + 4y + 3$ over $\boldsymbol{F}_7$, with $\deg(a) \leq 1, \deg(b) \leq 1$, where h is given modulo terms of total degree 4 and the term order in $A = \boldsymbol{F}_7[x, y]$ is total degree lexicographic with $x > y$. This example appeared originally in Buchberger *et al.* (1985) and later in Sakata (1990). By Theorem 5.1 the required solution is the minimal reduced solution with respect to $<_\omega$ defined by $\omega = (x, x)$, equivalently $\omega = (1, 1)$. Clearly, the condition of the corollary also holds so the required solution is minimal in M. It is straightforward to apply Algorithm 2.1: the terms are examined in the sequence $1\boldsymbol{e}_1, 1\boldsymbol{e}_2, y\boldsymbol{e}_1, y\boldsymbol{e}_2, x\boldsymbol{e}_1, x\boldsymbol{e}_2, \ldots$ and the first basis element is determined as soon as $x\boldsymbol{e}_2$ has been tested. We find that $(a, b) = (5y + 3, 5x + 5y + 1)$. Also, in the application of Algorithm 4.7 using the implementation suggested in Remark 4.8(ii) (using $<$ to define the sequence of ideals), the first element in M appears and is minimal modulo $I_\ell = \langle x^2, y^3, y^2x \rangle$. This is the minimal element in M and is the same as that found by Algorithm 2.1.

In the next example I is not generated by terms and, in addition, the corollary does not hold. Here the application is to inversion modulo a triangular set (Kapur and Lakshman, 1992).

EXAMPLE 5.4. Let $h = x^2yz^2 + xyz^2 + x^2z^2 + x^2yz + xz^2 + xyz + x^2z + x^2y + xz + xy + x^2 + x$ and determine the inverse (if it exists) of h in the algebra $\mathbf{F}_2[x, y, z]/I$ where $I = \langle x^3+x+1, y^3+y+1, z^3+z+1 \rangle$. The inverse $b = h^{-1}$ corresponds to the solution $(1, b)$ where $(1, b)$ satisfies $\mathrm{wtoc}(1, x^2y^2z^2, <)$ with $<$ total degree lexicographic with $x < y < z$ and hence is the minimal reduced solution of M with $<_\omega$ defined by $\omega = (x^2y^2z^2, 1)$. We find that all reduced terms of the form $\varphi\boldsymbol{e}_2$ are less than $1\boldsymbol{e}_1$. Algorithm 2.1 finds the following basis elements in the order given: $(0, x^3 + x + 1), (0, y^3 + y + 1), (0, z^3 + z + 1), (1, xy^2z^2 + y^2z^2 + xyz^2 + yz^2)$. The last of these is the minimal reduced solution. Note that its leading term is $1\boldsymbol{e}_1$ and that it is not the minimal solution. The inverse of h is therefore $xy^2z^2 + y^2z^2 + xyz^2 + yz^2$.

EXAMPLE 5.5. Another interesting application arises from a method of decoding certain geometric Goppa codes proposed in Porter *et al.* (1992) and Shen (1992). Without going into the details of the algebraic geometric background which lies outside the scope this paper, we may interpret their technique as follows.

Let $<$ be a fixed term order on $\mathcal{T}_1$ and write elements of $\mathcal{T}_1$ in the form $x^j = x_1^{j_1} \cdots x_n^{j_n}$. Let $u = (u_1, \ldots, u_n) \in \mathbf{N}_0^n$ be given and define a grading on $F[x_1, \ldots, x_n]$ by $\deg(x^j) = u \cdot j$. Define an order $<_u$ on $\mathcal{T}_1$ by $x^j <_u x^k$ if either $\deg(x^j) < \deg(x^k)$ (in $\mathbf{N}_0$) or $(\deg(x^j) = deg(x^k)$ and $x^j < x^k)$. It is easy to show that $<_u$ is a term order. The reader may refer to Becker and Weispfenning (1993, Section 10.2), for more details.

Next let $f \in F[x, y]$ where F is a finite field and the affine curve $f = 0$ is regular. For a certain geometric Goppa code C defined from f it is shown in Porter *et al.* (1992) that there exists a polynomial g such that the decoding problem for C is equivalent to the determination of a solution (a, b) of (1.1), with $I = \langle f, g \rangle$ zero dimensional, in which $\deg(b)$ is minimal subject to $\deg(a) - \deg(b) \leq s$ for a fixed positive integer s (associated with the curve). To solve this problem using Algorithm 2.1 we define a term order $<_2$ in $\mathcal{T}_2$ as follows. Let $<$ be total degree lexicographic order in $\mathcal{T}_1$ with $x < y$ and let $<_u$ be the term order in $\mathcal{T}_1$ defined above. Define $\varphi \boldsymbol{e}_i <_2 \psi \boldsymbol{e}_i$, for $i = 1, 2$, if and only if $\varphi <_u \psi$, and define $\varphi \boldsymbol{e}_1 <_2 \psi \boldsymbol{e}_2$ if either $\deg(\psi) - \deg(\varphi) \leq s$ or $(\deg(\psi) - \deg(\varphi) = s$ and $\varphi <_u \psi)$ and $\psi \boldsymbol{e}_2 <_2 \varphi \boldsymbol{e}_1$ otherwise. The reader may verify that this rather unwieldy definition is equivalent, in the formulation of Becker and Weispfenning (1993, Section 10.2), and Robbiano (1985) to defining $<_2$ in the algebra $F[x, y, z_1, z_2]$ via the matrix

$$\begin{pmatrix} 4 & 5 & 1 & 12 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

For a specific example from Shen (1992) we may take $F = F_{16}$, $u = (4, 5)$, $f = x^5 + y^4 + y$ (the Hermitian curve), $g = y^5$, $s = 11$ and $h = x^4 y^3 + x^4$. Then

$$1\boldsymbol{e}_1 <_2 x\boldsymbol{e}_1 <_2 \cdots <_2 y^2\boldsymbol{e}_1 <_2 1\boldsymbol{e}_2 <_2 x^3\boldsymbol{e}_1 <_2 \cdots <_2 y^3\boldsymbol{e}_1 <_2 x\boldsymbol{e}_2 <_2 \cdots.$$

Applying Algorithm 2.1 we examine the normal forms of the terms as far as $x\boldsymbol{e}_2$, at which point the required minimal degree solution (y, x) is determined. This agrees with that determined in Shen (1992) using a subresultant algorithm.

Finally, we give a more explicit example of Algorithm 4.7.

Example 5.6. (Fitzpatrick and Flynn, 1992) Let $h = 1 + x + y + x^2 + xy + y^2 + x^3 + y^3 \in \mathbf{F}_2[x, y]$, let I be the ideal generated by terms of total degree 4, and let the term order $<$ in $\mathcal{T}_1$ be total degree lexicographic with $x < y$. Define $<_\omega$ via the weight vector $\omega = (1, x)$ so that

$$1\boldsymbol{e}_1 <_\omega x\boldsymbol{e}_1 <_\omega 1\boldsymbol{e}_2 <_\omega y\boldsymbol{e}_1 <_\omega x^2\boldsymbol{e}_1 <_\omega x\boldsymbol{e}_\omega <_\omega \cdots$$

There are 10 iterations in the algorithm corresponding to the 10 monomials which are in normal form modulo I. These are displayed in the following table. The basis elements are always written in their correct order under $<_\omega$ and the term in $\mathcal{T}_1$ corresponding to the leading term is underlined. An asterisk indicates one of a pair with leading term of the form $x\varphi_q \boldsymbol{e}_k, y\varphi_q \boldsymbol{e}_k$ where the other has been omitted because its leading term is a multiple of another leading term.

x^0		x		y		x^2
$(\underline{1},0)$	1	$(\underline{x},0)$	1	$(1+x,\underline{1})$	1	$(1+x+\underline{y},1)$	1
$(0,\underline{1})$	1	$(1,\underline{1})$	1	$(\underline{y},0)$	1	$(\underline{x^2},0)$	1
		$(\underline{y},0)$	0	$(x^2,0)^*$	0	$(x+x^2,\underline{x})$	0
						$(y+xy,\underline{y})$	0

xy		y^2		x^3	
$(1+x+y+\underline{x^2},1)$	1	$(1+y,1+\underline{x})$	1	$(x+x^2+\underline{xy},x)$	1
$(x+x^2,\underline{x})$	1	$(x+x^2+\underline{xy},x)$	0	$(1+xy,1+x+\underline{y})$	0
$(x+x^2+\underline{xy},x)$	0	$(y+xy,\underline{y})$	1	$(y+xy+\underline{y^2},y)$	0
$(y+xy,\underline{y})$	0	$(y+xy+\underline{y^2})$	0	$(x+x^2+xy+\underline{x^3},x)$	0
$(y+xy+\underline{y^2})$	0	$(x+x^2+xy+\underline{x^3})^*$	0	$(x+xy,x+\underline{x^2})^*$	0

x^2y		xy^2		y^3	
$(1+xy,1+x+\underline{y})^\dagger$	0	$(1+xy,1+x+\underline{y})$	0	$(1+xy,1+x+\underline{y})$	0
$(y+xy+\underline{y^2},y)$	1	$(x+y+x^2+y^2+\underline{x^3},x+y)$	0	$(x+y+x^2+y^2+\underline{x^3},x+y)$	1
$(x+x^2+xy+\underline{x^3},x)$	1	$(x+xy,x+\underline{x^2})$	1	$(x^2+x^3+\underline{x^2y},x^2)$	0
$(x+xy,x+\underline{x^2})$	0	$(x^2+x^3+\underline{x^2y},x^2)$	0	$(xy+x^2y+\underline{xy^2},xy)$	0
$(x^2+x^3+\underline{x^2y},x^2)^*$	0	$(xy+x^2y+\underline{xy^2},xy)$	0	$(y^2+xy^2+\underline{y^3},y^2)$	0
		$(y^2+xy^2+\underline{y^3},y^2)$	0	$(x^2+x^2y,x^2+\underline{x^3})^*$	0

Note that the current minimal element is first equal to the minimal element at † as may be seen from the zero coefficients at the subsequent iterations. The basis resulting from the last step is

$$\{(1+xy,1+x+\underline{y}),(x^2+x^3+\underline{x^2y},x^2),(xy+x^2y+\underline{xy^2},xy),(y^2+xy^2+\underline{y^3},y^2),$$
$$(x^2+x^2y,x^2+\underline{x^3}),(x^2+xy+x^3+xy^2+\underline{x^4},x^2+xy)\}.$$

The corresponding reduced basis is

$$\{(1+xy,1+x+\underline{y}),(x^2+x^3+\underline{x^2y},x^2),(x+xy+\underline{xy^2},x+x^2)$$
$$(1+x+y+x^2+xy+y^2+x^3+\underline{y^3},1),(x^4,0),(x^3,\underline{x^3})\}$$

which is the same as that determined by reducing the basis given in Fitzpatrick and Flynn (1992, Example 3.2).

References

Adams, W. W., Loustaunau, P. (1994). *An Introduction to Gröbner bases*. Providence, RI: Amer. Math. Soc.

Becker, T., Weispfenning, V. (1993). *Gröbner bases*. New York: Springer-Verlag.

Buchberger, B., Krishnamurthy, E. V., Winkler, F. (1985). Gröbner bases, polynomial remainder sequences and decoding of multivariable codes. In N.K. Bose (ed.) *Multidimensional Systems Theory*, Dordrecht: Reidel, pp. 252–256.

Faugère, J.C, Gianni, P., Lazard, D., Mora, T. (1993). Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symb. Comp.*, **16**, 329–344.

Fitzpatrick, P. (1995). On the key equation. *IEEE Trans. Inform. Theory*, **41**, 1290–1302.

Fitzpatrick, P., and Flynn, J. (1992). A Gröbner basis technique for Padé approximation. *J. Symb. Comp.* **13**, 133–138.

Kapur, D., and Lakshman, Y. N. (1992). Elimination methods: an introduction. In Bruce Donald, Deepak Kapur, Joe Mundy, (eds) *Symbolic and Numerical Computation for Artificial Intelligence*, New York: Academic Press, pp. 45–89.

Möller, T., Mora, H. M. (1986). New constructive methods in classical ideal theory. *J. Alg.* **100**, 138–178.
Robbiano, L. (1985). Term orderings on the polynomial ring. In B. F. Caviness, (ed.) *EUROCAL '85, European Conference on Computer Algebra, Linz, Austria, Vol. II*, **204**, 513–517, Springer LNCS.
Robbiano, L. (1986). On the theory of graded structures. *J. Symb. Comp.* **2**, 139–170.
Porter, S. C., Shen, B., Pellikaan, R. (1992). Decoding geometric Goppa codes using an extra place. *IEEE Trans. Inform. Theory* **38**, 1663–1676.
Sakata, S. (1990). Partial realization of 2–D discrete linear system and 2–D Padé approximation and reduction of 2–D rational transfer function. *Proc. IEEE* **78**, 604–613.
Shen, B. (1992). Solving a congruence on a graded algebra by a subresultant sequence and its application. *J. Symb. Comp.* **14**, 505–522.

Originally received 19 July 1993
Accepted 28 January 1997